AO 106 (Rev. 04/10) Application for a Search Warrant

EC

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The A+ Self Storage Facility, specifically Unit 605 and Unit 611, located at 5960 E. Livingston Avenue in COlumbus, OH 43213 which is currently leased to Robert Gemienhardt, and any digital media located therein.

Case No. 2:22-mj-270

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein by reference

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251	Production of child pornography in interstate commerce
18 U.S.C. 2252/2252A	Receipt, distribution, and/or possession of visual depictions of a minor engaged in sexually explicit conduct and/or child pornography, in interstate commerce

The application is based on these facts:

See attached affidavit incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Jeremy Lindauer, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: April 14, 2022

City and state: Columbus, Ohio

Kimberly A. Johnson
United States Magistrate Judge

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO,
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:	)	**Case No:** 2:22-mj-270
	)	
The A+ Self Storage Facility, specifically Units 605 and 611, located at 5960 E Livingston Ave in Columbus, Ohio 43232 which is currently leased to Robert B. Gemienhardt, and any digital media located therein.	)	**Magistrate Judge:**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeremy Lindauer (Your Affiant), a Special Agent with the Federal Bureau of Investigation (FBI), Athens Resident Agency, being first duly sworn, hereby depose and state:

I. EDUCATION, TRAINING AND EXPERIENCE

1. I am a Special Agent (SA) with the Federal Bureau of Investigations (FBI) and have been since September of 2015. I am currently assigned to the Resident Agency in Athens, Ohio.
2. Prior to joining the FBI, I worked as a patrol officer for the Fishers Police Department in Fishers, Indiana, between 2008 and 2015. While there, I received training and experience in conducting many types of criminal investigations, including crimes against children. I was promoted to Field Training Officer for the department prior to leaving to accept a position as Special Agent for the FBI in 2015. Within the FBI, I was first assigned to the Joint Terrorism Task Force in New York City, where I conducted and assisted in complex terrorism investigations across the globe. I was transferred to the Athens Resident Agency in September of 2020, where my responsibilities expanded to include investigating criminal violations relating to child exploitation and child pornography violations, including the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A.
3. As a SA with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have not withheld any evidence or information which would negate probable cause. I have set forth only the facts necessary to establish probable cause for a search warrant for the A+ Self Storage Facility, specifically Unit 605 and Unit 611, located at 5960 East Livingston Avenue in Columbus, Ohio 43232, which is currently leased to Robert B. GEMIENHARDT (hereinafter referred to as the **SUBJECT PREMISES**).
5. The **SUBJECT PREMISES** to be searched is more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A – the production, distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the entirety of the **SUBJECT PREMISES**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed; if that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce; or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
7. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual

depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.

8. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

9. The term "child pornography"[1], as it is used in 18 U.S.C. § 2252A, is defined pursuant to 18 U.S.C. § Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.

10. The term "sexually explicit conduct", as used in 18 U.S.C. §§ 2251 and 2252, is defined pursuant to 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to 18 U.S.C. §

---

1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

2256(2)(B), "sexually explicit conduct" when used to define the term child pornography, also means "(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person."

11. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."
12. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."
13. "Graphic" when used with respect to a depiction of sexually explicit conduct, means that viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10)).
14. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
15. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).
16. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in

[2] The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

17. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
18. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES, THE INTERNET

19. I know from my training and experience that computer hardware, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.
20. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.
21. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be

accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

22. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

23. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or

video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

24. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses3 and other information both in computer data format and in written record format.

25. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service

providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

26. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

27. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

28. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or

"footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

29. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a) Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b) Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an

operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

31. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU) as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

VI. INVESTIGATION AND PROBABLE CAUSE

32. In February 2022, your affiant received information pertaining to an individual by the name of Robert B. GEMIENHARDT who was believed to have distributed child pornography online after having sustained a previous conviction for a crime against a minor child. GEMIENHARDT was currently residing in Hocking County, Ohio. Your affiant subsequently obtained numerous reports and spoke with officials from the Hocking County Sheriff's Office and the Columbus Division of Police regarding the current and previous investigation of GEMIENHARDT that had been conducted thus far.

33. On or about December 30, 2021, a CyberTipLine report was submitted to the National Center for Missing and Exploited Children (NCMEC) by Kik Messenger services regarding the uploading of child pornography to the Kik account associated with the username xxxbigdxxx. According to the information that was provided by Kik, between the dates of November 14, 2021, and November 23, 2021, fourteen files depicting child sexual abuse material were transmitted over the Kik messenger servers via the target Kik account. The CyberTipLine report indicated that seven of the fourteen files were identified using the MD5 hash matching method. Copies of the uploaded files were included with the CyberTipLine report along with information pertaining to the IP address utilized to access the account at the time the suspect files were transmitted and a registered email for the Kik account, which was redrobin_mgr@hotmail.com. A summary of some of those images is as follows:

- One image titled 8baa9a90-fd30-46b8-a5f9-aa6a8575bf1e.jpg depicting a nude pubescent female with adult male penis inserted into her anal cavity and a white substance covering her genitalia.

- One image titled 5fd7f2a5-7de5-4ad9-ad49-eee8e6754d29.jpg depicting two nude pubescent females preparing to kiss each other with their nude genitalia exposed to the camera.
- One image titled 00cdf857-72f2-42fb-b7ff-614b9dd9cc57.jpg depicting a pubescent female with her underwear pulled down, exposing her nude genitalia.

34. The investigation revealed that the IP address used to upload the child sexual abuse material was geolocated to Hocking County, Ohio. More specifically, the IP address resolved to the internet service provider Spectrum with a subscriber name of Carrie DANIELS at the address of 1167 Charles Street in Logan, Ohio.

35. On or about February 22, 2022, the Hocking County Sheriff's Office (HCSO) in Logan, Ohio received the NCMEC CyberTipLine report from the Ohio Internet Crimes Against Children Task Force (ICAC). In the initial investigation into this address, an open-source search on the Ohio sex offender registry revealed Robert B. GEMIENHARDT had listed the address of 1167 Charles Street in Logan, Ohio as his residence. GEMIENHARDT was listed as a Tier I sex offender. HCSO drove by the Charles Street address of GEMIENHARDT and observed numerous children's toys outside the residence. HCSO later confirmed that four minor females resided at that address as well including five-year-old JANE DOE ONE, twelve-year-old JANE DOE TWO, fifteen-year-old JANE DOE THREE and seventeen-year-old JANE DOE FOUR.

36. In accordance with the terms of his sex offender registration obligations, GEMIENHARDT was asked to meet with law enforcement from the HSCO. During that meeting, after being advised of his Miranda rights, GEMIENHARDT admitted that his Kik username was xxxbigdxxx, and that he had used his email address redrobin_mgr@hotmail.com to register his Kik account. GEMIENHARDT also confirmed that he had used Kik to view child pornography in the past and further admitted to viewing and possessing images of minor children and disseminating those photos online. At that point, GEMIENHARDT was arrested for a violation of Ohio Revised Code 2907.322(A)1 (Pandering Sexually Oriented Matter Involving a Minor).

37. Subsequent to GEMIENHARDT's arrest, HCSO obtained numerous search warrants which ultimately led to the recovery of two cell phones and one desktop computer belonging to GEMIENHARDT, to include GEMIENHARDT's personal Samsung Galaxy Note 10+ cell phone.

38. A forensic extraction of the Samsung Galaxy Note 10+ was completed by the FBI who had been in contact with HCSO and assisting with the investigation. A subsequent review of that extraction revealed thousands of text messages between GEMIENHARDT and Carrie DANIELS discussing all four JANE DOES in a sexual manner. More specifically, numerous messages were recovered detailing the efforts of GEMIENHARDT and DANIELS to groom each JANE DOE to engage in sexual acts with both GEMIENHARDT and DANIELS. The following is an excerpt of the conversations between GEMIENHARDT (RG) and DANIELS (CD) occurring on December 30, 2020:

RG: The way JANE DOE THREE keeps grabbing your boobs.....the idea of you tasting her pussy
CD: You want me to?
RG: The idea is naughty and hott
RG: It would be hot to see you both naked touching eachother
RG: The idea of you pleasing her
CD: Tell me more

39. Another conversation occurring on February 16, 2021, detailed the continuing discussions of JANE DOE THREE

RG: I wanna see her touch you wet pussy as you touch hers
CD: Too bad we didn't get to see it last night
RG: So close
CD: It really was. I think she wants to see you naked
RG: [surprised emoji]
CD: She wants you to streak
RG: You wanna show her? How would you do it
CD: Would you like her seeing?
RG: I was asking if you wanna show her cock
CD: She has seen before...
RG: Massage my legs while I lay on my back
CD: Yeah
RG: I know you would slide your hands in my boxers to rub me down as i got harder
RG: Which means she would see you tech rubbing my cock
RG: Then just depends if you pull it out at all
RG: Wonder how she would react
CD: Nice!
CD: She would look. She looks at your ass a lot
RG: She watch you stroke me off
RG: Make me explode

CD: Not sure about that
RG: So if i was gonna cum you would cover me up
CD: Play it by ear
RG: Would you keep rubbing and make me cum... or would you stop
CD: It would be hard to stop
RG: Mmmm
CD: you've seen her tits a few times
RG: Yes she hasn't been shy... lol
CD: Has she shown you her pussy yet?
RG: No
CD: Maybe she was trying last night??
RG: Not sure
CD: Never know
RG: Hott seeing u touch her

40. The conversation continued into April 2021 revealing more detailed set-ups of leading JANE DOE THREE to more advanced sexual activities, up to and including GEMIENHARDT touching and rubbing JANE DOE THREE's breasts and vagina. The following is an excerpt of a conversation occurring on April 17, 2021:

RG: Let's make JANE DOE THREE really wet tonight
CD: Oh yeah?
RG: Let's see if she sleeps with us tonight
CD: She seems pretty flirty tonight
RG: [winking emoji][winking emoji]
CD: Did you see how wet her shorts are in the bathroom?
RG: No
RG: Is it nice
CD: Yes it is
RG: Tonight lets see if she will go in the middle
RG: You suck her tits nice and slow again
CD: If she's up for it. Yes!
RG: I'll see how wet she is...see if she is interested in playing
RG: Maybe tonight u kiss that pussy
CD: Be careful though
RG: I will
RG: Im inside there all the time
CD: Lips touching lips while we kiss

41. Your affiant also noted a conversation occurring November 24, 2021, between GEMIENHARDT and DANIELS in which GEMIENHARDT distributed to DANIELS an approximately 31-second video depicting himself masturbating and ejaculating into the underwear of JANE DOE FOUR. In response to receiving the video from

GEMIENHARDT, DANIELS indicated that she showed the video to JANE DOE ONE. The following conversation then ensued:

RG: What did JANE DOE ONE say watching me cum
CD: Commented teh (sic) panties were JANE DOE FOUR's
RG: She knew the panties
CD: Yeah
RG: What all did she say
CD: Not much. Said she wasn't looking at your pee pee
RG: She say anything about cum on panties
CD: No
RG: She needs covered in cum
RG: On her pussy
RG: U wish we could be openly sexual with all 6 of them
RG: I loved when u used to grab my hand and put it on her pussy
RG: So naughty
CD: Very naughty
RG: Put the tip of my cock on her and explode all on and in her lil hole
CD: Whoops! Yummy

42. In addition to the text messages recovered relating to each JANE DOE, numerous images which depicted JANE DOE ONE were recovered which depicted JANE DOE ONE and Carrie DANIELS. The following is a brief summary of the images seized from GEMIENHARDT's phone it relates to JANE DOE ONE:

- One image depicting JANE DOE ONE's right hand inserted into the nude vagina of DANIELS. The metadata on this image indicates that it was produced on June 14, 2020 using the digital media device attributed to DANIELS and then distributed to GEMIENHARDT that same day. At the time the image was produced, JANE DOE ONE would have been three years of age.

- One image depicting JANE DOE ONE laying on a bed fully nude, with her legs spread exposing her vagina and anus. JANE DOE ONE was pictured lying in-between the legs of DANIELS, who was also nude from the waist down, and DANIELS nude vagina is directly next too JANE DOE ONE's buttocks. The metadata on this image indicates that it was produced on June 16, 2020 using the digital media device attributed to DANIELS and then distributed by DANIELS to GEMIENHARDT who last viewed or accessed the image on June 28, 2020. At the time the image was produced, JANE DOE ONE would have been three years of age.

- One image depicting JANE DOE ONE nude from the waist down, laying on a bed with a sexual device in between her legs. In the image, DANIELS is depicted lying next to JANE DOE ONE, also engaged in acts of masturbation with a

different sexual device. The metadata on this image indicated that it was last viewed or accessed on August 25, 2020 and was therefore produced sometime before that day making JANE DOE ONE approximately three to four years of age in the image.

43. Based on the images recovered on GEMIENHARDT's phone, on March 4, 2022, DANIELS was arrested by HCSO for a violation of Section 2907.02 of the Ohio Revised Code (Rape). Upon her arrest, a blue Samsung Galaxy S10 was seized from DANIELS and a search warrant for that device was obtained. A forensic extraction of DANIEL's device revealed the following as it related to GEMIENHARDT:

- One image, depicting JANE DOE ONE engaged in the lascivious display of genitalia. In the image, the nude vagina of DANIELS and the nude penis of GEMIENHARDT are also depicted and JANE DOE ONE is positioned between the two of them. The metadata associated with this image indicates that it was last viewed or accessed June 13, 2020 and therefore produced before that date making JANE DOE ONE approximately three to four years of age in the image.
- One image depicting JANE DOE ONE's hand wrapped around the nude penis of GEMIENHARDT. The metadata associated with this image indicates that this image was last viewed or accessed on August 28, 2020, and therefore produced before that date making JANE DOE ONE approximately three to four years of age in the image.

44. The forensic examination of GEMIENHARDT's Samsung Galaxy Note which has been completed thus far has also revealed approximately 1,100 images of what reasonably appeared to be child sexual abuse material. Those images include prepubescent males and females, some as young as toddler age, engaged in nudity, oral sex, masturbation, or other sexual activity with other adults. Review of the forensic extraction, as well as other investigation into GEMIENHARDT's online child exploitation activities, remains ongoing.

45. Your affiant has also confirmed that on July 6, 2021, GEMIENHARDT was convicted of Sexual Imposition pursuant to Section 2907.03 of the Ohio revised Code out of Franklin County Municipal Court in Franklin County, Ohio. According to Columbus Division of Police reports obtained by your affiant, the victim in that case was approximately five years of age at the time of the incident.

46. On April 7, 2022, a complaint and arrest warrant for GEMIENHARDT was signed by a US Magistrate Judge in the Southern District of Ohio. GEMIENHARDT was arrested the following day.

47. On April 10, 2022, a relative of GEMIENHARDT, herein after WITNESS ONE, reached out to the FBI National Threat Operations Center (NTOC) regarding information related to a digital media device located in **SUBJECT PREMISES.**

48. As a follow up to the NTOC report, on April 12, 2022, your affiant interviewed WITNESS ONE. WITNESS ONE informed your affiant that she received a letter from GEMIENHARDT which had been written while GEMIENHARDT was in the Southeastern Ohio Regional Jail after his Hocking County arrest in February of 2022. Your affiant learned that in that letter, GEMIENHARDT told WITNESS ONE that WITNESS ONE could go to GEMIENHARDT's storage units to retrieve some items, also giving WITNESS ONE permission to cut the locks if needed. In addition, GEMIENHARDT asked that WITNESS ONE retrieve a file bin and briefcase for safekeeping while GEMIENHARDT was incarcerated.

49. According to WITNESS ONE, GEMIENHARDT had two storage units in his name, which your affiant now knows to be the **SUBJECT PREMISES**. WITNESS ONE informed your affiant that he/she went to the **SUBJECT PREMISES** to obtain children's clothing items, toys, and other necessities. In addition, WITNESS ONE was accompanied to the **SUBJECT PREMISES** by WITNESS TWO who located the briefcase and file bin as referred to by GEMIENHARDT within the **SUBJECT PREMISES**. WITNESS TWO then observed that inside the briefcase was a laptop computer. Both WITNESS ONE and WITNESS TWO were familiar with the criminal complaint against GEMIENHARDT and were concerned that the laptop had also been used by GEMIENHARDT in the commission of his criminal activities. WITNESS ONE and WITNESS TWO left the laptop in the **SUBJECT PREMISES** and contacted the FBI via the NTOC.

50. On April 13, 2022, your affiant interviewed the Area Manager for Advantage Consulting Management, which is the company that oversees management of the **SUBJECT PREMISES**. The manager informed your affiant that the **SUBJECT PREMISES** is currently leased to GEMIENHARDT. Your affiant also learned that **SUBJECT**

PREMISES had been paid for by GEMIENHARDT through March 31, 2022 and that GEMIENHARDT was past-due on his April payment.

51. Based on the information that had been gathered to date by your affiant, including forensic examination of digital media devices recovered in this case belonging to both GEMIENHARDT and Daniels, in conjunction with statements made by WITNESS ONE, combined with your affiant's belief that GEMIENHARDT likely possess the characteristics common to individuals with a sexual interest in minors, as described below, your affiant believes that there is probable cause that the **SUBJECT PREMISES** contains evidence of child pornography and child exploitation activities.

VII. SEARCH METHODOLOGY TO BE EMPLOYED

52. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of items described in Attachment B found at **SUBJECT PREMISES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:

    1. Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment B;
    2. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in Attachment B;
    3. Surveying various files, directories and the individual files they contain;
    4. Opening files in order to determine their contents;
    5. Scanning storage areas;
    6. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
    7. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

53. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in children and who produce, distribute, and receive child pornography:

a) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c) Those who have a sexual interest in children and who produce, distribute, and receive child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. More recently, however, it has become more common for people who have a sexual interest in children to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence

on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

d) Likewise, those who have a sexual interest in children and who produce, distribute, and receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e) Those who have a sexual interest in children and who produce, distribute, and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and sometimes maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f) Those who have a sexual interest in children and who produce, distribute, and receive child pornography rarely are able to abstain from engaging in sexual exploitation of children or child pornography activities for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

54. When images and videos of child pornography are produced and stored on computers and related digital media, forensic evidence of the production, distribution, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

55. Based upon the conduct of individuals who have a sexual interest in children and who produce, distribute, and receive child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, that they rarely are able to abstain from child pornography activities for a prolonged period of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even

years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of production, distribution and possession of child pornography is currently at **SUBJECT PREMISES**.

IX. CONCLUSION

56. Based on all the forgoing factual information, there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252 and 2252A have been committed and that evidence, fruits and instrumentalities of these offenses will be found within **SUBJECT PREMISES** listed in Attachment A, which is incorporated herein by reference. Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of **SUBJECT PREMISES** described in Attachment A, and the seizure of the items described in Attachment B.

Jeremy Lindauer
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 14th day of April, 2022.

Kimberly A. Johnson
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PLACE TO BE SEARCHED

The place to be searched is the location described below, including any and all computer-related devices or digital media located therein.

Storage Units 605 and 611 located at A+ Self Storage Facility, 5960 E Livingston Ave in Columbus, OH 43232 are described as garage-like storage units with blue colored rolling overhead doors, and with the numbers "605" and "611" posted on the wall above the doors respectively. Due to the fact that the facility was closed and the particular units to be searched were inaccessible at the time of the photograph, the subject premises will be similar in appearance to the units depicted above, but the **SUBJECT PREMISES** are not specifically depicted.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A (production, possession, receipt, and distribution of child pornography), those violations involving Robert B. GEMIENHARDT, including:

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, USB/thumb drives, SD cards, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica;
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs;
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, and electronic messages,) pertaining to the production, possession, receipt, or distribution of child pornography;

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to digital files, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by cellular phone or computer, any child pornography;

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications related to the sexual abuse or exploitation of minors;

7. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service;

8. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information;

9. Any and all visual depictions of minors, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation;

10. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct;
11. Any and all cameras, film, videotapes or other photographic equipment;
12. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed, posted, and/or traded;
13. Any Internet or cellular telephone communications (including email, social media, etc.) with minors;

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.